

CENTRAL INTELLIGENCE AGENCY

WASHINGTON, D.C. 20505

OGC REVIEW
COMPLETED

18 March 1977

MEMORANDUM FOR: PRM/NSC-11 Subcommittee Members

FROM: Anthony A. Lapham
General Counsel

SUBJECT: CIA Comments on Draft Unauthorized Disclosure
Legislation and Related Matters

1. This memorandum pertains to the first item on the agenda distributed at last week's organizational meeting of the PRM/NSC-11 subcommittee chaired by Mr. Harmon. That agenda called for comments by 16 March on a draft criminal statute, copies of which were also distributed at the meeting, relating to the unauthorized disclosure of national security information, and on other possible civil or criminal approaches to the overall problem addressed by the draft statute.

The Context

2. The basic existing statute dealing with unauthorized disclosure of national security information is the Espionage Act, enacted in 1917 and largely unchanged over the last 60 years, and particularly two sections of that Act, 18 U.S.C. §§793 and 794. ^{1/} These provisions are vague and clumsy in their

^{1/} There are a number of other provisions, in the Espionage Act and other statutes, but none are of such general application. So, for example, the statutory inventory would include the so-called photographic statutes (18 U.S.C. §§795 and 797 and 50 U.S.C. §781, outlawing sketches or photographs of certain military installations or equipment), 18 U.S.C. §798 (which covers cryptographic information), 18 U.S.C. §952 (which relates to disclosure of foreign diplomatic codes), the so-called restricted data statute, 42 U.S.C. §§2271-81 (applicable to information concerning atomic energy and weapons), and 50 U.S.C. §783 (making criminal the disclosure by Government employees of classified information to foreign agents). Other statutes become applicable only in wartime. All the statutes in this group have limited utility in that they are directed to rather specialized circumstances that do not often occur.



wording. For example, they describe the category of information to which they relate as "information relating to the national defense," which quite conceivably could include everything from the most vital national secrets to the daily stock market reports. Some of these uncertainties have been sorted out by judicial interpretation, so that it is now settled that at a minimum the provisions apply, and are constitutional as applied, to those activities commonly associated with "spying," e.g., selling secrets to the Soviets. It remains unclear, however, whether as a matter of law these provisions could be applied to other very different forms of unauthorized disclosure, such as the publication of books or leaks to the press. It is extremely doubtful that the provisions were intended to have application in such situations, and as a matter of historical fact, leaving aside the unsuccessful Ellsberg prosecution and possibly one or two other cases, they never have been so applied. ^{2/} The draft statute would pick up where the Espionage Act appears for all practical purposes to leave off and would extend criminal sanctions to acts of disclosure in situations not characterized by dealings with foreign agents or powers.

3. In other than espionage situations, there obviously are critically important public policies favoring the free flow of information and ideas necessary to informed public discussion and debate, and at the same time there are well-known or at least widely suspected bureaucratic tendencies to overclassify, undoubtedly fed by the slipperiness of the classification standards, and occasional efforts to conceal embarrassing mistakes, or something worse, behind bogus national security claims, all of which are factors that produce hostility and skepticism when it comes to proposed

^{2/}Under current Justice Department procedures, unauthorized disclosures of national security information, in other than espionage situations, are almost never even investigated, let alone prosecuted. Apart from a natural reluctance to proceed in such situations, stemming from the absence of any clearly applicable statute, the principal stumbling block standing in the way of investigations is the Department of Justice practice of insisting on an advance commitment that the compromised information, which as disclosed is very apt to be fragmentary and only partially accurate, will be declassified for purposes of prosecution. Essentially a commitment to declassify is a commitment to officially confirm in accurate terms, and probably to augment, the information involved, and thus the more sensitive the information, the more painful the declassification decision required to be made. The upshot is that the worst and most damaging leaks are the ones least likely to be investigated.

secrecy legislation. Beyond these barriers lie the fundamental constitutional precepts with a direct bearing on legislation in this field, namely, the First Amendment prohibition against the enactment of any law abridging freedom of speech or press, the mandate, rooted in the Fifth Amendment, that legislated norms of conduct be expressed in terms that are reasonably certain and definite, especially where criminal penalties are attached, and the procedural guarantees surrounding the judicial process, not to mention the rules of discovery.

The Key Elements

4. In view of the opposing forces and values, it seems to us that any proposed legislation must be as finely drawn as possible if it is to have any decent chance of survival in both the Congress and the courts. Further, it seems to us that any proposed bill must have the following essential features:

- (a) A clear definition of the class of persons that would be exposed to liability.
- (b) A clear definition of the type of information that would be covered -- that is, as to which communication would be restricted.
- (c) A clear definition of the kind of communications that would be restricted -- that is, the circumstances in which the disclosures of restricted information would constitute an unlawful act.
- (d) A provision establishing a mental standard of culpability -- that is, the intent element of the offense.
- (e) Provisions creating a procedure for prompt and independent review, upon request by a person subject to the law's restraints, of official determinations that particular information requires protection against disclosure.
- (f) Provisions that eliminate or at least minimize the need to publicly disclose sensitive information, over and above the information compromised by the unauthorized disclosure, in order to establish the commission of an offense.
- (g) Sanctions effective for the purpose of deterring the conduct declared to be unlawful.

The Draft Statute

5. In form, the draft statute would amend Chapter 93 of Title 18 of the United States Code by adding a new section 1924, entitled "Unauthorized

Disclosure of Classified Information." Chapter 93 contains an assortment of criminal provisions relating to the conduct of public officers and employees, and since the draft statute is in keeping with that theme, we think its placement in Chapter 93 would be appropriate.

6. Generally speaking, as we understand the basic scheme, the draft statute would make it an offense for any member of a class consisting of all those persons authorized to possess or control classified information to communicate such information to any person not a member of that class. We have several reservations about that basic scheme, and we have organized our comments in the order of the considerations that we deem to be of key significance, as outlined in paragraph 4 above.

7. Subsections (a) and (b)(2) must be read together to determine the coverage of the bill, as to persons. Subsection (a) provides:

(a) Whoever, being or having been in authorized possession or control of classified information or material, or being or having been an officer or employee of the United States, a member of the Armed Forces of the United States, a contractor of the United States Government, an employee of such a contractor, or an employee of Congress, and in the course of that relationship acquires knowledge of classified information or material, knowingly communicates such information or material to a person not authorized to receive it shall be fined not more than \$10,000 or imprisoned not more than five years.

Under this language, the affected class consists of specifically enumerated categories of persons (members of the Armed Forces, etc.), to the extent they acquire knowledge of classified information in the course of government employment or employment by a government contractor, plus anyone else formerly or presently "in authorized possession or control of classified information or material." The latter catchall category is explained by subsection (b)(2), which provides:

(b)(2) A person is deemed to be authorized to possess, control, or receive classified information or material, (A) if he is an officer or employee of the United States, a member of the Armed Forces of the United States, a contractor of the United States Government or an employee of such contractor, with a security clearance of the same characterization as the classified information or material, (B) if he is a Member of

Congress, an employee of Congress, or an officer or employee of the Judicial branch of the United States Government, or (C) if he has been authorized in writing to possess, control, or receive classified information by an officer of the United States appointed by the President.

8. As we see it, subsections (a) and (b)(2) are redundant in some respects and inconsistent in others. So, for example, looking just to subsection (a), one would conclude that employees of Congress, but not members of Congress, are part of the affected class. However, looking to subsection (b)(2), as one must in order to find the meaning of the phrase "[w]hoever, being or having been in authorized possession or control of classified information or material," as that phrase is used in subsection (a), the conclusion to be drawn is that the affected class includes members as well as employees of Congress. The confusion comes about because subsection (b)(2) introduces the concept of a class of authorized recipients of classified information, without however making clear the function of that concept, and the net result is that the bill lacks a plain and definite statement indicating who is, and who is not, exposed to liability.

9. The preferable approach in our judgment would be to devote a single subsection to a delineation of the affected class, rather than squeezing the definition into multi-purpose subsections such as (a) and (b)(2). As to the proper dimensions of that class, we think that if anything the net may have been cast too widely in the draft statute and that consideration should be given to narrower definitions of the class. In addition, we note that if the affected class is defined to include all former government employees who may have had access to classified information, it will necessarily include at least some newspapermen, and therefore, assuming that publication is one of the forms of communication to which the bill applies, a direct albeit limited control will be placed on what information a newspaper can publish without a threat of prosecution.

(b) The type of information that would be restricted

10. Under subsection (a) the restraint on communication would extend to all classified information, which is defined in subsection (b)(1) to mean:

...any information, (A) regardless of its origin, that is marked or designated pursuant to the provisions of a statute or an executive order, or a regulation or rule issued pursuant thereto, as information requiring protection against unauthorized disclosure for reasons of national security, or (B) that was furnished to the United States by a foreign government or international organization and was designated by such foreign government or international organization as requiring protection against unauthorized disclosure.

The essential effect of this language is to incorporate by reference Executive Order 11652, and the implementing National Security Council directive of 17 May 1972, governing the procedural and substantive aspects of classification, declassification, and downgrading of national security information. We doubt the wisdom of this approach. In the first place, E.O. 11652 and the implementing NSC directive are subject to amendment at the stroke of the President's pen, so that the adoption of subsection (b)(1) would leave the President free to fix and revise the standards of criminal liability as he might see fit, a prerogative that Congress would almost certainly not want to endorse even assuming that such a sweeping delegation of power would be constitutionally valid. In the second place, the importation into the bill of the executive classification system, in its entirety, would open up the possibility that genuinely sensitive information might go unprotected due to some procedural irregularity in the manner of its classification (classifying official not identified on the face of a document, etc.). And in the third place, it seems to us that the universe of classified information is quite simply too large, and encompasses such a great variety of material of so many different degrees of importance to the national security, as to make impractical the idea of extending criminal sanctions to the unauthorized disclosure of all such information.

11. Here again we would favor a narrower and more discriminating approach, along the lines of the sources and methods legislation that CIA has previously supported and that was introduced as H.R. 12006 in the last Congress. We also believe that the standards against which information is to be measured to determine whether it falls into the restricted category should be spelled out in the bill rather than identified by reference to E.O. 11652 or any other existing OGC 25X1 executive branch directives.

OGC25X1

OGC25X1

(c) The kind of communications that would be restricted

12. As already noted, the conduct declared unlawful by subsection (a) is the communication of restricted information by any person authorized to possess it to any person not authorized to receive it. Assuming the intent element of the offense is clarified, this strikes us as workable, although we believe that "communicates" should be a defined term and that the definition should include the acts of furnishing, transmitting, or otherwise making available [restricted information to an unauthorized person], as well as the act of publication.

(d) The intent element

13. Under subsection (a) an offense is committed if a person acts "knowingly," However, it is unclear with reference to what fact or facts a person must have knowledge. Must he know that he is a member of the affected class, or that he is dealing with an unauthorized recipient, or that the character of the information is such as to bring it within the law's definition of restricted data, or some combination or all of these facts. That matter requires clarification. Similarly, since it presumably is not the intention to make punishable an inadvertent act (as for example a communication with a person reasonably believed to be an authorized recipient), willfulness should probably be added as an element of the offense. In the same vein, consideration should be given to some sort of a general exclusion for communications made in the course of the performance of official duties, this to take care of the not uncommon situations in which high-ranking officials disclose classified information during news briefings, etc.

(e) Review procedures

14. Subsection (c)(1) provides:

(c) It shall not be an offense under this section:

(1) If at the time of the disclosure there did not exist a review through which the defendant could obtain review of the lawfulness of the classification of the information or material. Any failure to declassify information or material pursuant to such review shall be agency action adversely affecting the individual requesting the declassification.

As we understand this provision, it would require a showing, presumably to a judge as a preliminary pre-trial matter rather than to a jury as an element of the government's proof at trial, that there existed at the time of the alleged unauthorized disclosure an administrative procedure through which the defendant could have sought and obtained review of the information involved to determine whether it could be classified. It is our further understanding that this provision would create a judicial remedy under the Administrative Procedure Act, 5 U.S.C. §§701, et seq., in the event a review requested and conducted pursuant to the required administrative procedure resulted in a refusal to declassify.

15. Subsection (c)(1) is obviously designed to enhance the appeal and acceptability of the draft statute, by providing safeguards against arbitrary classification decisions by executive branch officials. More than that, this subsection is woven into the fabric of the statute and, in conjunction with subsection (e), discussed below, it would play a major role in shaping the offense of unauthorized disclosure by eliminating, in circumstances where the defendant did not avail himself of the review procedure, any requirement of proof that the classification of the information was valid and justified.

16. In principle we have no objection to a two-tier system of administrative and judicial review. Indeed such a system exists today in connection with FOIA requests, more particularly those requests as to which the Agency considers or claims the exemption set forth in 5 U.S.C. §552(b)(1), which provides that the FOIA does not apply to matters that are "(A) specifically authorized under criteria established by an Executive order to be kept secret in the interest of national defense or foreign policy and (B) are in fact properly classified pursuant to such Executive order." And in addition to the internal Agency and external judicial reviews that are available to an FOIA requester, in cases where the documents subject to the request are classified, there is an existing avenue of appeal to the Interagency Classification Review Committee, an entity established pursuant to Section 7 of E. O. 11652 to monitor the implementation of that Order.

17. While we are comfortable with the concept embodied in subsection (c)(1), we would like to know more about the characteristics of the administrative review procedure that it would require. For that matter, we think the required procedures should be described in some detail in the bill, both in order to enable agencies to determine whether their existing procedures satisfy the requirement and in order to head off potential arguments by defendants that the opportunity for review afforded them was not the sort of opportunity contemplated by the bill. There is also a point relating to the comparability of the standards of judicial review available under the APA on the one hand and the FOIA on the other that needs to be discussed.

(f) Provisions limiting the proof necessary to establish the commission of an offense

18. Subsection (e) provides:

(e) In any prosecution under this section where the defendant did not seek review of the lawfulness of the classification of the information or material, it shall not be an element of the offense that the information or material was lawfully classified at the time of the disclosure.

This provision rules out the validity of classification as an element of the offense, in cases where the defendant did not pursue the administrative and judicial remedies mandated by subsection (c)(1). It is not clear whether, although the government need not establish the validity of classification in these circumstances, an accused could still defend on the grounds that the information in question was not properly classified. In our opinion that issue should be ruled out as a defense as well as an affirmative part of the government's case. Apart from that consideration, the provision seems to us to represent a promising approach to the problems of proof often associated with prosecutions involving the unauthorized disclosure of sensitive information.

(g) Sanctions

19. Subsection (a) provides that an offense would be punishable by a fine of not more than \$10,000 or imprisonment for not more than five years. These penalties are adequate and sufficiently flexible in our view, assuming the appropriateness of criminal sanctions.

(h) Other

20. Subsection (c)(3) provides:

(c) It shall not be an offense under this section:

(3) To disclose any information already in the public domain, but to disclose additional details or information confirming previously unconfirmed information, which details or information remain classified, continue to be an offense under this section.

We regard this provision as undesirable. Whether information is in some sense in the public domain, and how it came to be in the public domain (i.e., by official statements or otherwise), are questions that clearly have a bearing on the continuing validity of the classification of that information, and that being true those questions should certainly be open for consideration in the review process to which subsection (c)(1) refers. But those questions have no evident relevance at a trial in which the validity of classification is foreclosed as an issue, as is contemplated by subsection (e).

Anthony A. Lapham

A Bill

To prohibit the unauthorized disclosure of classified information.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

That title 18, United States Code, be amended by (a) adding the following new section:

"§ 1924. Unauthorized disclosure of classified information.

"(a) Whoever, being or having been in authorized possession or control of classified information or material, or being or having been an officer or employee of the United States, a member of the Armed Forces of the United States, a contractor of the United States Government, an employee of such a contractor, or an employee of Congress, and in the course of that relationship acquires knowledge of classified information or material, knowingly communicates such information or material to a person not authorized to receive it shall be fined not more than \$10,000 or imprisoned not more than five years.

"(b) For purposes of this section:

"(1) The term 'classified information or material' means any ^{or information} information, (A) regardless of its origin, that is marked or designated pursuant to the provisions of a statute or an executive order, or a regulation or rule issued pursuant thereto, as information requiring protection against unauthorized disclosure for reasons of national security, or (B) that was furnished to the United States by a foreign government or international organization and was designated by such foreign government or international organization as requiring protection against unauthorized disclosure.

"(2) A person is deemed to be authorized to possess, control, or receive classified information or material, (A) if he is an officer or employee of the United States, a member of the Armed Forces of the United States, a contractor of the United States Government or an employee of such contractor, with a security clearance of the same characterization as the classified information or material, (B) if he is a Member of Congress, an employee of Congress, or an

officer or employee of the Judicial branch of the United States Government, or (C) if he has been authorized in writing to possess, control, or receive classified information by an officer of the United States appointed by the President.

"(c) It shall not be an offense under this section:

"(1) If at the time of the disclosure there did not exist a review procedure through which the defendant could obtain review of the lawfulness of the classification of the information or material. Any failure to declassify information or material pursuant to such review shall be agency action adversely affecting the individual requesting the declassification.

"(2) To disclose any information to a Member of Congress or a court of the United States.

"(3) To disclose any information already in the public domain, but to disclose additional details or information confirming previously unconfirmed information, which details or information remain classified, continue to be an offense under this section.

"(d) A person not authorized to possess, control, or receive classified information or material is not subject to prosecution for conspiracy to commit an offense under this section, or as an ^{abettor} ~~aid~~, or accomplice under sections 2 and 3 of title 18, United States Code, in the commission of an offense under this subsection, unless he became possessed of such information in the course of a relationship with the United States Government as described in subsection (a).

"(e) In any prosecution under this section where the defendant did not seek review of the lawfulness of the classification of the information or material, it shall not be an element of the offense that the information or material was lawfully classified at the time of the disclosure.

"(f) This section shall not be deemed to derogate from any civil remedies the United States may have."



Approved For Release 2002/05/20 : CIA-RDP80-00473A000300040007-2

WASHINGTON, D. C. 20301

DD/A Registry
File 84M

MAR 12 1977

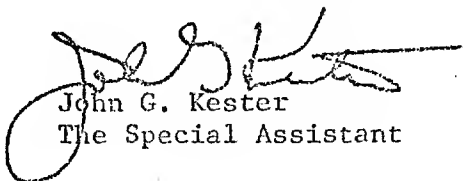
DD/A Registry
77-1426

Executive Registry
77-35618

MEMORANDUM FOR THE VICE PRESIDENT
THE SECRETARY OF STATE
THE SECRETARY OF THE TREASURY
THE ATTORNEY GENERAL
THE DIRECTOR, OFFICE OF MANAGEMENT AND BUDGET
UNITED STATES REPRESENTATIVE TO THE UNITED NATIONS
ASSISTANT TO THE PRESIDENT FOR NATIONAL SECURITY AFFAIRS
DIRECTOR, CENTRAL INTELLIGENCE AGENCY
ADMINISTRATOR, ENERGY RESEARCH AND DEVELOPMENT ADMINISTRATION

SUBJECT: Presidential Review Memorandum/NSC-11 - Intelligence Structure and Mission

The Secretary of Defense has designated Mr. David E. McGiffert, Assistant Secretary of Defense for International Security Affairs-designate, as the focal point within the Department of Defense for all activities relating to PRM/NSC-11. He will be assisted by Mr. Thomas K. Latimer, Principal Deputy Assistant Secretary of Defense for Intelligence and Mr. Leonard Niederlehner, Acting General Counsel and such other persons as Mr. McGiffert may designate. All correspondence and inquiries should be directed to the Office of the Assistant Secretary of Defense for International Security Affairs. The office telephone numbers are 695-4351, 697-9729 and 697-2788.


John G. Kester
The Special Assistant

cc:

Secretaries of the Military Departments
Chairman, Joint Chiefs of Staff
Assistant Secretaries of Defense
General Counsel
Director, Defense Intelligence Agency
Director, National Security Agency
Deputy Assistant Secretary of Defense (Administration)
Inspector General for Defense Intelligence

100M 100000

55

Approved For Release 2002/05/20 : CIA-RDP80-00473A000300040007-2



STAT

Approved For Release 2002/05/20 : CIA-RDP80-00473A000300040007-2

Next 1 Page(s) In Document Exempt

Approved For Release 2002/05/20 : CIA-RDP80-00473A000300040007-2